A Step-by-Step Guide to Secured Zoom Meetings (Zoom-Bombers Beware!)

The objective of this guide is to reduce the possibility of problematic participants sharing unwanted comments or content. While we appreciate public participation, it is important to sustain an environment for responsible civic engagement.

Use this guide to lock down your Zoom meeting and prevent "Zoom bombing." Follow the steps **before**, **during**, and **after** the meeting. Also included are short role descriptions and a tiny script you can copy into an invite so that people know each person's responsibilities.

Important Note for Sunshine Law Boards

Boards and commissions subject to Hawai'i's Sunshine Law should be aware that not all of the security practices in this guide may be fully applicable to their meetings. Because Sunshine Law requires that remote meeting links be posted publicly in advance, some preventive measures - such as restricting access only to authenticated users - may not be feasible. Additionally, while boards cannot preemptively block members of the public from attending, they may remove individuals who engage in disruptive behavior and prevent those removed individuals from rejoining the same meeting.

These guidelines are intended to help enhance meeting security while still aligning with Sunshine Law requirements. Boards should apply the recommendations that are compatible with open-meeting obligations and consult their counsel or the Office of Information Practices (OIP) if uncertain. You may contact OIP's Attorney of the Day with questions about the Sunshine Law's requirements at oip@hawaii.gov or 808-586-1400

Important Note About Technical Instructions

Portions of this guideline outline specific instructions in navigating throughout the platform. Due to regular occurring software updates, some steps may alter from what is written. We recommend visiting the Enterprise Technology Services (ETS) Tips to Prevent Zoom Bombings page for the most recent updates: https://servicedesk.hawaii.gov/support/solutions/articles/21003336752-Tips-to-Prevent-Zoom-Bombings

Assign roles (who does what)

- **Host (you / meeting owner)**: Schedules the meeting, sets security options, able to lock the room, remove participants, and end the meeting.

- **Moderator (gatekeeper)**: Monitors the waiting room, admits people in the meeting, removes problematic participants, mutes/unmutes participants as needed, turns off participant video if needed. The host and moderator can be the same person.
    - ***Instructions:*** *Navigate to assigned through Participants → More → Make Co-Host*
- **Facilitator (meeting conductor)**: In many cases, the chair of the meeting, runs the agenda, calls on speakers, manages time, handles Q&A and polls.
    - The facilitator can be the host/ moderator, however facilitating the meeting while performing the gatekeeping tasks of the moderator, is, a lot to handle. Having a separate person for each role is highly recommended.

Tip: Assign **both** a Moderator and a Facilitator for important meetings. A Moderator manages security/disruptions whereas a Facilitator manages content/flow.

Before the meeting (do these steps every time)

1. **Schedule the meeting with a unique meeting ID**
    - When scheduling, **do not** use your Personal Meeting ID (PMI). Let Zoom generate a random meeting ID for that event.
2. **Require a meeting password**
    - Turn on the password option and include the password only in the calendar invite (not on public social media).
3. **Enable the Waiting Room**
    - Turn on the Waiting Room option so you can admit participants one-by-one or in small groups.
4. **Turn on Meeting Authentication if appropriate**
    - Require sign-in with a Zoom account (or SSO) if attendees are internal or you want an extra barrier. This step may not be necessary for a public meeting.
5. **Limit screen sharing by default**
    - Set "Who can share?" to **Host Only.** (You can allow others in the meeting when needed.)
6. **Disable "Join before host"**

- Prevent attendees from entering before the host to avoid unmanaged presence.

7. **Disable "Allow removed participants to rejoin"**
    - Prevent banned participants from returning.
8. **Disable file transfer and remote control**
    - Turn off file transfer and remote control to reduce accessibility for participants unless there is a need for this.
9. **Turn off annotation (or limit it to host)**
    - Prevent strangers from scribbling on your screen share.
10. **Consider using a Webinar license**
    - For large, public events, webinars provide more control (attendees are unable to unmute nor share their screen).
11. **Update your Zoom client & recommend attendees to have the latest updated Zoom software**
    - Use the latest version to get security patches.
12. **Send meeting details securely**
    - Put link + password in a calendar invite or internal email. **Do not** post the raw meeting link publicly.

Quick security checklist to use when you start the meeting

1. Assign co-host(s) to Moderator & Facilitator.
2. Require all participants to identify themselves with first and last names.
3. Admit participants from the Waiting Room intentionally.
4. Mute all participants on entry (Participants → Mute All).
5. Confirm screen sharing permission is Host Only.
6. Confirm chat settings (see below).
7. If everyone is present, **Lock Meeting** (Participants → More → Lock Meeting).

In-meeting actions if something goes wrong

1. **Remove the disruptive participant**
    - Participants → hover name → Remove
    - If they try to return, ensure "Allow removed participants to rejoin" is **off**
2. **Stop their video and audio** (if needed)
    - Participants → More → Stop Video / Ask to Unmute (or Mute)
3. **Put them in Waiting Room** (if you want to temporarily isolate)
    - Participants → hover name → Put in Waiting Room
4. **Lock the meeting** to stop additional entries (after you've admitted everyone)
5. **Turn off screen sharing** instantly (Host controls → disable participant sharing)
6. **Suspend participant activities**: If severe, use "Suspend Participant Activities" (that disables video, audio, screen share, chat, reactions) or end meeting for all
7. **Report the disruptive user to Zoom** after the meeting if content was abusive

---

Recommended chat & participant settings (during scheduling or while in meeting)

- **Chat**: Limit chat to "Host and co-hosts only" or disable private chat to prevent link sharing
- **File transfer**: OFF
- **Annotation / Whiteboard**: Host Only or OFF
- **Renaming**: Disable participants from renaming themselves if you want verified names
- **Mute on entry**: ON

Short scripts you can copy/paste

- **Invite blurb (calendar invite):**

  Please do not share this meeting link publicly. This meeting uses a password and Waiting Room — you will be admitted from the Waiting Room. If you join late, please wait to be admitted.

- **At meeting start (host says):**

  Aloha — quick housekeeping: everyone is muted on entry. Please keep your video on or off at the facilitator's instruction. If you need to speak, click 'Raise Hand'. The moderator will admit people from the Waiting Room and assist with issues. Thanks!
